

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

A.P., R.E.A., and K.G., on behalf of
themselves and all others similarly situated,

Plaintiffs,

v.

ZETA GLOBAL CORPORATION and ZETA
GLOBAL HOLDINGS, CORPORATION,

Defendants.

x

:

:

:

:

:

:

:

:

:

:

:

:

:

x

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs A.P., R.E.A., and K.G. (collectively, “Plaintiffs”), on behalf of themselves and all others similarly situated, bring this Class Action Complaint against Defendants Zeta Global Corporation and Zeta Global Holdings, Corporation (collectively, the “Defendant” or “Zeta”), for violations of federal and state laws set forth herein in connection with Defendant’s unlawful acquisition, aggregation, collection, retention, resale and use for profit of sensitive information from January 1, 2019 through the present day (“Class Period”).

Plaintiffs make the following allegations based upon personal knowledge as to themselves, as well as upon information and belief as well as investigation of counsel as follows:

INTRODUCTION

1. In an increasingly digital world, Americans who use internet-connected devices rely on the internet for numerous different tasks which, at one point, could only be accomplished in person. From utilizing digital storefronts, seeking medical information, and using online banking systems, much of what consumers do on the internet creates thousands of individual data points of highly sensitive information. Woven together, these data points of highly sensitive information add up to a fabric detailing who a person is on an intimate level which could never be replicated but for the use of the internet.

2. With this in mind, consumers who use the internet have a fundamental expectation of privacy when they engage in online activity. This includes the expectation that consumers do not expect corporations to engage in surreptitious, systematic, and wide-spread surveillance of their online activity.

3. With the understanding that much of the world’s commerce is now conducted online, digital retailers and service providers prioritize transacting in consumer information so that they can best target specific potential customers over consumers’ privacy rights. As such, and

unknownst to consumers themselves, this has given rise to digital marketplaces that collate, organize, purchase, and sell in consumer data.

4. These marketplaces, as well as the intrinsic value of online consumer data, has given rise to a new industry of technology companies which operate to acquire personalized data used to identify and target consumers across digital channels. One of the largest corporations in this new industry is Defendant, Zeta. According to Defendant:

Zeta is an AI-Powered Marketing Cloud whose vision is to make sophisticated marketing simple. The Zeta Marketing Platform (ZMP), relaunched in 2019, leverages advanced artificial intelligence (AI) and trillions of consumer signals to make it easier for marketers to acquire, grow, and retail customers more efficiently and effectively. The ZMP is differentiated in that it is the largest omnichannel marketing platform with identity data at its core.

5. Defendant's business is predicated on collecting data from consumers without their knowledge so that purchasers of consumers' data profiles can target potential customers for goods and services through advertising channels, such as through email, social media, websites ad spaces, chat applications, connected TV devices and video popups. According to Defendant, they maintain at least 245 million profiles on American consumers. The profiles consist of "a comprehensive mix of proprietary, partner, and publicly available data... includ[ing] an average of more than 2,500 attributes per individual" and this data, which is not aggregated or anonymized and is tied to individual internet users, consists of demographic information, behavioral data, psychographic data, transactional information, and other preferences (the "PII"). This PII is acquired either through website tracking code called "pixel" technologies on third-party websites, through data publishers or other data aggregators who sell this type of sensitive information.

6. As of 2025, Defendant has nearly 2,000 companies who purchase this PII. According to Defendant, the key benefit to using ZMP is that it "lets you reach virtually every U.S. consumer with high impact omnichannel campaigns powered by AI." In essence, ZMP's

core function is to run the PII of nearly every single U.S. consumer who uses the internet through AI in order to best profile and target them with omnichannel advertising campaigns.

7. To be clear, Defendant's entire business model relies on being able to violate privacy rights and collect PII from unwitting consumers. Defendant admits as such. For example, in Defendant's Annual Report for 2024, Defendant flags "new tools" to protect consumer privacy, as well as evolving regulatory restrictions, as an existential risk to the viability of the business as well as a potential "harm [to Zeta's] operating results and financial conditions."

8. Defendant's violations of federal, state and common law have the intended purpose of violating consumer privacy. Among the hundreds of millions of victims of Defendant's invasive privacy practices are consumers who use at least one of the thousands of businesses which transact in PII with Defendant.

9. Plaintiffs, on behalf of themselves and Class members, bring this proposed class action on behalf of all consumers whose PII was acquisition, aggregation, collection, retention, resale and use for profit by Defendant for redress of the injury and damages suffered and continue to suffer by reason of Defendant's continuing unlawful conduct as well as injunctive relief to cease Defendant's various violations of law.

JURISDICTION and VENUE

10. This action arises under the federal, state, and common law. Plaintiffs and Class members seek relief under the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*), including: declaratory, equitable and injunctive relief, as well as a measure of damages (including actual damages, punitive damages and statutory damages), disgorgement of profit, costs of suit, pre- and post-judgment interest and reasonable attorneys' fees and costs, as permitted by statute. With respect to state and common law violations, Plaintiffs and Class members seek relief for

violations of the California Invasion of Privacy Act, violations of New York's General Business Law § 349 and unjust enrichment, including: injunctive relief, as well as a measure of damages (including punitive or exemplary damages, as well as statutory and trebled damages), disgorgement of profit into a constructive trust, costs of suit, pre- and post-judgment interest and reasonable attorneys' fees, as this Court deems necessary and proper.

11. *Subject Matter and Supplemental Jurisdiction.* Plaintiffs bring this Action under the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*) such that subject matter jurisdiction is proper under 28 U.S.C. §§ 1331, 1332(d), 1337(a) and 1367. This Court has federal question jurisdiction under 28 U.S.C. §§ 1331 and 1337 because Plaintiffs assert claims arising under federal law. Additionally, this Court has supplemental jurisdiction over Plaintiffs' state and common law claims under 28 U.S.C. § 1367 because all of their claims arise from the same facts and circumstances and form part of the same case or controversy.

12. Additionally, this Court also has subject matter jurisdiction over Plaintiffs' state law and common law claims under the Class Action Fairness Act of 2005 (28 U.S.C. § 1332(d)) ("CAFA"). This Court has subject matter jurisdiction under CAFA because the amount in controversy exceeds the sum of \$5,000,000 (exclusive of costs and interest), there are more than 100 putative members of the Class and minimal diversity exists between the litigants, as one or more of the Class members is a different citizen than Defendant. Namely, Plaintiff K.G. is domiciled in California whereas Defendant is headquartered in New York.

13. *Personal Jurisdiction.* This Court has personal jurisdiction over Defendant because its principal place of business is located in New York. Additionally, this Court has personal jurisdiction over Defendant because Defendant is registered to do business in New York, a

substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in New York, including Defendant's interception and use of Plaintiffs' PII.

14. *Venue.* Venue is proper in this District under 28 U.S.C. §1391(b), (c) and (d), because a substantial portion of the conduct described in this Class Action Complaint was carried out in this District. Further, Defendant maintains substantial business operations in this District.

PARTIES

PLAINTIFFS

Plaintiff A.P.

15. Plaintiff A.P. is and was domiciled in Suffolk County, New York during the Class Period.

16. During the Class Period, Plaintiff A.P. used numerous online retailers' storefronts and services, including those of Defendant's business clients such as Apple and Yahoo!, which implemented Defendant's identifiers and tracking software.

17. For each of these services, Plaintiff A.P. created an account and logged-in using his email address and other information. Unbeknownst to Plaintiff A.P., Defendant intercepted his PII from the online services he used, processed this information and created and/or supplemented a digital profile maintained by Defendant.

18. Many of Defendant's client's websites also use online tracking technology. Through this technology, Defendant's profile of Plaintiff A.P. was unknowingly populated with specific pages he viewed or the content of his searches. Defendant processed this data and stored it on its Amazon Web Services, Google Cloud and Microsoft Azure storage systems to target Plaintiff A.P. with its business clients' ads.

19. Defendant used its technology to track Plaintiff A.P. across the internet, creating approximately 2,500 data points on Plaintiff A.P., including on the web, mobile devices, connected TVs and other platforms. When Plaintiff A.P. visited websites or used other services operated by a participating business client, Defendant used tracking technology to recognize Plaintiff A.P. as the intended recipient of a targeted advertisement.

20. The reason for this was because Defendant and its business clients profited from this data collection apparatus; furthermore, Defendant's profile on Plaintiff A.P. facilitated real-time bidding for digital ad spaces (on websites, applications, Connected TVs, and elsewhere online) that would ultimately be served to him specifically.

21. Plaintiff A.P. did not consent to Defendant intercepting his PII, assigning and using unique identifiers to track him across internet-enabled services and devices, or interception his private communications for profit.

Plaintiff R.E.A.

22. Plaintiff R.E.A. is and was domiciled in Suffolk County, New York during the Class Period.

23. During the Class Period, Plaintiff R.E.A. used numerous online retailers' storefronts and services, including those of Defendant's business clients such as Synchrony Bank and Yahoo!, which implemented Defendant's identifiers and tracking software.

24. For each of these services, Plaintiff R.E.A. created an account and logged-in using her email address and other information. Unbeknownst to Plaintiff R.E.A., Defendant intercepted her PII from the online services she used, processed this information and created and/or supplemented a digital profile maintained by Defendant.

25. Many of Defendant's client's websites also use online tracking technology. Through this technology, Defendant's profile of Plaintiff R.E.A. was unknowingly populated with specific pages she viewed or the content of her searches. Defendant processed this data and stored it on its Amazon Web Services, Google Cloud and Microsoft Azure storage systems to target Plaintiff R.E.A. with its business clients' ads.

26. Defendant used its technology to track Plaintiff R.E.A. across the internet, creating approximately 2,500 data points on Plaintiff R.E.A., including on the web, mobile devices, connected TVs and other platforms. When Plaintiff R.E.A. visited websites or used other services operated by a participating business client, Defendant used tracking technology to recognize Plaintiff R.E.A. as the intended recipient of a targeted advertisement.

27. The reason for this was because Defendant and its business clients profited from this data collection apparatus; furthermore, Defendant's profile on Plaintiff R.E.A. facilitated real-time bidding for digital ad spaces (on websites, applications, Connected TVs, and elsewhere online) that would ultimately be served to her specifically.

28. Plaintiff R.E.A. did not consent to Defendant intercepting her PII, assigning and using unique identifiers to track her across internet-enabled services and devices, or interception her private communications for profit.

Plaintiff K.G.

29. Plaintiff K.G. is and was domiciled in Los Angeles County, California during the Class Period.

30. During the Class Period, Plaintiff K.G. used numerous online retailers' storefronts and services, including those of Defendant's business clients such as Apple, which implemented Defendant's identifiers and tracking software.

31. For each of these services, Plaintiff K.G. created an account and logged-in using her email address and other information. Unbeknownst to Plaintiff K.G., Defendant intercepted her PII from the online services she used, processed this information and created and/or supplemented a digital profile maintained by Defendant.

32. Many of Defendant's client's websites also use online tracking technology. Through this technology, Defendant's profile of Plaintiff K.G. was unknowingly populated with specific pages she viewed or the content of her searches. Defendant processed this data and stored it on its Amazon Web Services cloud to target Plaintiff K.G. with its business clients' ads.

33. Defendant used its technology to track Plaintiff K.G.. across the internet, creating approximately 2,500 data points on Plaintiff K.G., including on the web, mobile devices, connected TVs and other platforms. When Plaintiff K.G. visited websites or used other services operated by a participating business client, Defendant used tracking technology to recognize Plaintiff D.G. as the intended recipient of a targeted advertisement.

34. The reason for this was because Defendant and its business clients profited from this data collection apparatus; furthermore, Defendant's profile on Plaintiff K.G. facilitated real-time bidding for digital ad spaces (on websites, applications, Connected TVs, and elsewhere online) that would ultimately be served to her specifically.

35. Plaintiff K.G. did not consent to Defendant intercepting her PII, assigning and using unique identifiers to track her across internet-enabled services and devices, or interception her private communications for profit.

DEFENDANTS

Defendant Zeta Global Corporation

36. Defendant Zeta Global Corporation is a Delaware corporation headquartered in New York with its principal place of business located at 3 Park Avenue, 33rd Floor, New York, New York 10016.

Defendant Zeta Global Holdings, Corporation

37. Defendant Zeta Global Holdings, Corporation is a Delaware corporation headquartered in New York, with its principal place of business located at 3 Park Avenue, 33rd Floor, New York, New York 10016. Defendant Zeta Global Holdings, Corporation is publicly traded, with its common stock trading on the New York Stock Exchange under the ticker symbol “ZETA.”

38. Defendant, initially called XL Marketing Corporation, was founded in 2007 by former Apple chief executive officer and Pepsi president, John Sculley, as well as David A Steinberg, founder and chief executive officer of InPhonic and Sterling Cellular.

39. Defendant knowingly and intentionally developed a complex system of unique identifiers and tracking mechanisms to surveil Plaintiffs and Class members across internet-connected devices, despite knowing these types of identifiers were at odds with users’ basic expectations of digital privacy.

40. Defendant new that its identifiers and profiles on users circumvented existing privacy protections, because, initially, Defendant advertised its data collection apparatus as being entirely opt-in for consumers. However, recently, Defendant removed mentions of its opt-in data collection system in Annual Reports – which led to consternation and subsequent litigation by its shareholders.

41. Defendant offers its services to websites, mobile applications, advertisers, data brokers and other downstream purchasers of consumer PII. Defendant knowingly and intentionally used its identifiers, various data collection systems, and the resulting PII it obtained to profile online users and facilitate targeted advertisements for profit.

FACTUAL ALLEGATIONS

Background of User Tracking

42. Over the last decade, consumers have become substantially more conscious of their online privacy as the internet has become an increasingly pivotal tool for all facets of human existence. This consciousness has been reinforced by persistent data breaches of consumers' sensitive information as well as the ubiquitous and uniquely American experience of being microtargeted by online advertising.

43. While no federal law protected Americans from these concerns, and a patchwork of state laws only narrowly insulated users from online privacy issues, the only recourse for most consumers was to demand more data security mechanisms from the technology platforms themselves. In response to this, hardware developers like Apple and Google integrated new protections into their devices to adapt to consumer preferences for more adept privacy-preserving mechanisms. This, naturally, was to the benefit of Apple and Google: (1) the changes in preferences meant that more consumers would buy their privacy-centric products and (2) Apple and Google could insulate itself from others attempting to acquire the very data that the online advertising industry craved.

44. Consequentially, this shift in consumer preferences harms the preexisting digital advertising industry which relied on usurping user data by any means necessary. Advertisers in the digital world heavily relied on various tracking mechanisms (like advertising identifiers and

third-party cookies) to specifically identify unique individuals who use products and services (as well as similar products and services) in order to serve targeted advertisements to these individuals.

45. While these changes benefited consumers, the multibillion-dollar online advertising apparatus reviled at the changes, and immediately sought ways around the moat Apple and Google attempted to create not just for their consumers, but for the data that they could then keep for themselves.

46. A new industry, the data aggregation industry, has emerged to fill the void that digital advertisers wished to address due to specifically to Google and Apple's conduct, and, generally, the desire of consumers to maintain a reasonable expectation of privacy in the digital world the very same way they would in the physical world.

The Rise of the Data Aggregator

47. The last five years alone have shown the importance of occupying digital retail space for providers of products and services. This is especially so when accounting for the onset of COVID-19 in March of 2020. In the year prior to COVID-19, American consumers spent about \$500 billion making online purchases; in the decade since, Americans now spend about \$1.3 trillion annually over the internet. Sales numbers are anticipated to approach \$2 trillion by the end of 2029.

48. Against this backdrop, retailers selling products and services over the internet feel increasing pressure to be able to have data which allows them to target not just subgroups of consumers (*e.g.*, age ranges, gender, general geographic information and basic financial status) but individual users themselves. This has led to a powerful role of data aggregators in digital spaces. Rather than placing generic advertisements to anonymous, aggregated groups of potential customers, retailers now prioritize the access that data aggregators give them to individuals

themselves. And not only are these individuals identifiable, but many data aggregators provide thousands of data points on each consumer which are highly sensitive.

49. This unique opportunity is what changed the digital data industry's focus from consumer privacy to customer centricity.

Zeta's Business

50. Founded in 2007, Defendant describes itself as “a leading AI-powered omnichannel data-driven cloud platform that provides enterprises with consumer intelligence and marketing automation software. We empower our customers to target, connect and engage consumers through software that delivers personalized marketing across all addressable channels, including email, social media, web, chat, Connected TV [] and video, among others.”

51. With respect to what Defendant offers to nearly 2,000 consumer-facing business customers, Defendant states, “[o]ur Generative AI (GenAI)-driven marketing solutions enable brands to personalize experiences at every scale, measure impact with precision and optimize marketing spend to increase return on investment.”

52. The core of Defendant's business is called the Zeta Marketing Platform, or ZMP.

53. Using AI, ZMP functions as a marketing platform that uses the identity and identity affiliated data in order to best target specific consumers. According to Defendant on ZMP's capabilities, “[l]everaging GenAI and machine learning, the ZMP processes billions of structured and unstructured data signals to predict consumer intent, optimize messaging and drive personalized messaging across all channels.” The way that ZMP does this is by extracting information from interactions with a customer's marketing channels (such as a third-party business' website, mobile application or social media) using various types of technology such as tracking code (*e.g.* pixel tracking) as well as a third-party business' application programming

interface (“API”) that connects a business customer’s sources of data with ZMP so that ZMP can collect and retain it before it is fed through Defendant’s algorithm.

54. According to Defendant, ZMP is built on the following ‘four pillars’:

55. Defendant’s Data Set. Defendant claims to have data sets of profiles of more than 245 million individuals in the United States, with over 535 million individuals globally. Each of these half a billion profiles is constructed is through a “comprehensive mix of proprietary, partner and publicly available data.” On average, a profile is enriched with over 2,500 attributes per individual, including demographic, behavioral, psychographic, transactional, or other preference data.

56. This data is consumed at an incredible rate: with over one trillion data points ingested by ZMP on a monthly basis. Either taken individually or as part of a larger profile, this is the type of data which an online consumer would expect that they have a reasonable expectation over – especially in light of the fact that this data is not anonymous.

57. Defendant’s AI Engine. The way that ZMP can collect such significant amounts of data is through “GenAI, machine learning, natural language processing and predictive AI.” According to Defendant, Defendant can leverage AI, technology, and proprietary data within ZMP to be able to:

- a. Seamlessly collect and ingest structured and unstructured data into the ZMP;
- b. Detect PII and apply data governance in accordance with business, state and federal rules and regulations;
- c. Quickly and reliably analyze key consumer attributes and signals;
- d. Identify consumer intent by running sophisticated algorithms to analyze data;

- e. Cluster related concepts and prioritize actionable insights to create intent-based graphs;
- f. Create audiences comprised of individuals or affinity-driven clusters scored based on intent;
- g. Forecast experience-based outcomes at both an individual and audience level;
- h. Personalize content to make experiences more relevant for the consumer and profitable for the enterprises;
- i. Create channel and content recommendations to optimize marketing performance;
- j. Enable ZMP users to create GenAI agents and workflows, which chain discrete tasks together for automations;
- k. Determine intent of a ZMP user using GenAI and recommend next actions; and
- l. Leverage GenAI for the creation of campaigns, creative audiences, experiences, data onboarding processes and analysis of analytics.

58. This means that, unbeknownst to consumers, their PII is being trusted by some entity they have never even heard of to AI systems in order to be protected and then repackaged in a way which also makes it commodifiable.

59. Defendant's Omnichannel Engagement. In order for ZMP to effectively find consumers for its business customers, it integrates into third party sources who then take possession of the data in order to “deploy [] targeted marketing systems through a wider range of channels, devices and formats, all within a single platform.” According to ZMP, this process enables “customers to improve how they identify and engage the modern consumer who is using multiple devices and platforms (e.g., mobile, website, applications social media, connected TV and email).”

60. A major concern for the Plaintiffs and Class members is what happens to the data after it leaves the custody of Defendant's ZMP. While business customers may use the data it collects to ascertain who their potential consumers may be, it also gives access to untold amounts of unknown end-users who can use the same data for other purposes.

61. Defendant's Data Performance Optimization. The final pillar of Defendant's ZMP platform is the use of AI to deploy predictive models and machine learning that display as insights for the business customer to optimize returns on investment related to targeting advertising.

How ZMP Works

62. Various types of consumer-facing businesses use ZMP to best target potential clients for their respective businesses. ZMP does this by intercepting granular access to users to provide "a single, comprehensive view of [] customers and prospects, their buying behaviors and their brick-and-mortar and digital retail experiences."

63. First, ZMP assigns two ZMP-generated IDs which are "present for every client and will always be generated." These two types of IDs are called a "BSIN" identifier and a "ZYNC_ID."

- a. BSIN – According to ZMP, BSIN is a unique identifier that the ZMP system creates per profile. Every single profile in ZMP gets a BSIN. The website's unique identifier is tied to the BSIN, which is created by an API associated with the respective website.
- b. ZYNC_ID – According to ZMP, a ZYNC_ID is assigned by a line of code on a website (called a Zync Container Tag) and is then assigned to each person who is on that specific website. While the ZYNC_ID usually stays the same for a respective website user, it can change if the user switches devices or if they clear

browser cookies. However, ZMP is capable of reidentifying users with the existing ZINC_ID.

64. With the help of these two types of basic identifiers who identify the profiles of users themselves, ZMP's Identity Manager Service can assign records to specific profiles. Additionally, ZMP can enable a retailer to "consolidate disparate records into a distinct customer and household identifier based on name, a client key they maintain [and other information]." An example of this type of identifying code captured by ZMP while on a retailers' website appears as follows:

```
1  {
2    "customer_id": "CUST123456",
3    "client_key": "CKEY789012",
4    "hh_id": "HH987654",
5    "loyalty_number": "LOYAL3210",
6    "email": "johndoe@example.com",
7    "email_md5": "e13743a7f1db7f4246badd6fd6ff54ff", // MD5 hash of "johndoe@e:
8    "email_sha256": "2dc9f3b5e3e555b5adfd91aae3c3f083b298a08e4862f9f7cfb6a88244"
9  }
```

65. As a consumer continues to use a respective retailer's website for products and services, ZMP continues to collect more information which is even more sensitive than an identifier and rudimentary contact data, including name, address, and even the consumer's children's demographic information:

```

1  {
2      "first_name": "John",
3      "last_name": "Doe",
4      "gender": "Male",
5      "children": [
6          {
7              "age": 5,
8              "gender": "Female",
9              "name": "Emily"
10         },
11         {
12             "age": 7,
13             "gender": "Male",
14             "name": "Michael"
15         }
16     ],
17     "address_line_1": "1234 Elm Street",
18     "address_line_2": "Apt 5B",
19     "city": "Anytown",
20     "state": "Stateville",
21     "country": "USA",
22     "zip": "12345",
23     "other_address": {
24         "address_line_1": "5678 Oak Street",
25         "address_line_2": "Suite 12",
26         "city": "Othertown",
27         "state": "Stateplace",
28         "country": "USA",
29         "zip": "67890"

```

66. The more granular the data collected on a respective consumer, the more value that the specific subset of information holds. For example, ZMP is able to obtain other forms of purchase information that, prior to advanced data aggregation, would have been impossible to consolidate into a larger profile. The utility of this data, at a superficial level, is to provide ZMP's business customers with a profile of what information a consumer might purchase or be interested in. Once these simple connections are made and consolidated into their profile, ZMP can offer the information to businesses seeking to target consumers looking for those types of products:

JSON


```


1  {
2      "resource_type": "product",
3      "resource_id": "E_2M891AB",
4      "First Seen": "01/01/2023",
5      "Last Updated": "8 hours ago",
6      "Modified Date": "01/01/2023",
7      "Published Date": "02/01/2023",
8      "Description": "A versatile shoe for both casual and formal occasio
9      "age": "01/2023",
10     "brand": "ElegantFootwear",
11     "categories": "Men, Formal, Casual, Bestsellers, Clearance, Leather
12     "color": "Black",
13     "gender": "male",
14     "in_stock": false,
15     "offer_price": 50,
16     "price": 100,
17     "segment": "Adult",
18
19 }

```


67. Through the collection of thousands of data points, and in concert with ZMP's AI processing, Defendant can create a user-friendly profile for businesses to access specific consumers and have a considerable amount of PII on those users. For example, a ZMP business customer can access each of its ZMP consolidated profiles on a general page, then have PII displayed in a manner which gives the business customer significant information as to whether a specific customer could be converted into a viable client or repeat client.


68. For example, these profiles appear as follows:








Ross Geller
New York, New York, 10013, US



Contact

ross.geller@smithsonian.com 

0734e9ad-da44-4c00-908e-c8e8a51f78c... 


1da0686b-3858-464a-aaa1-28e6d1ec60... 

More 



Identifiers


ZMP Identifiers


User ID

ross.geller 

Email

ross.geller@smithso... 

More 


Key Properties

age

41

city

New York

date_of_birth

12-May-80

education

Ph.D.

ethnicity

American

marital_status

Divorced

occupation

Direct Response Of...

profession


Paleontologist

state

New York

zip

10013


Reachable Channels

☐ Programmatic
☐ Email
☐ Mobile

☐ Social
☐ CTV

69. Beyond just these profiles, Defendant also offers add-on information (if paid for by the ZMP subscriber) that includes the interests of a particular online user, an AI-based scoring chart for the likelihood that an online user falls into a certain demographic, as well as top activities

that the online user has taken recently – such as purchase information, new online subscriptions and returns of purchases.

70. Taken together, all this PII is highly sensitive. And, with over 2,500 different data points on each consumer, it barely scratches the surface as to what information ZMP might have stored beyond what is publicly known.

71. ZMP contains specific information which, unbeknownst to consumers, is made available to Defendant's business customers. Specifically, ZMP contains a system called Zeta Audiences, which create profiles based on data "segments created by selecting/combining various attributes available from Zeta's collection of proprietary audience data." The subcategories collected on each consumer for which Defendant maintains a profile (which is nearly every single online consumer in the United States) includes:

- a. Online Content Consumption: The online content consumption/behavioral data category which includes online digital audiences that demonstrate an intent to convert into various product categories.
- b. Visitation: Visitation data captures real-world movement by tracking device locations through mobile application and GPS navigation systems. It provides insights into where consumers go and how often they visit specific locations.
- c. Transaction: The transaction data category includes audiences that have been observed to have completed a transaction within the listed categories allowing you to target users that have shown explicit interest in listed areas.
- d. Financial & Household: Financial and Household data segments provide insights into individuals based on financial health indicators, household characteristics, property ownership and related lifestyle attributes.

- e. Demographics: Demographic data audiences group people by general population characteristics, such as age, gender, ethnicity, or income.
- f. Multicultural Data: Uses Natural Language Processing, census data and cultural signals to identify ethnic and country-of-origin segments under four main umbrellas: White/Non-Hispanic White, African American, Hispanic, and Asian.
- g. Propensities: Propensity audiences include customers with various brand, product, or service affinities.
- h. Psychographic: Psychographic audiences include customers whose behaviors align with particular personalities, values, and attitudes.
- i. TV Engagement: TV engagement audiences include various types of television viewers and their levels of content consumption.
- j. Firmographic: Firmographic audiences provide a single, consolidated view of the professional attributes of a target audience, such as job title and industry, company name, company age, company revenue, and company size.

72. According to Zeta's 2023 Annual Filing, Zeta's audience segments are even further reaching than what it states on its own website. For example, Zeta collects information on individual consumers including their political preferences, religious identity, LGBTQ+ status and specific health conditions.

73. Using all this sensitive information, ZMP is able to process it so that algorithms can make additional categorizations and determinations. These assumptions allow ZMP to provide its business customers with audiences of identifiable individuals which can be targeted for specific lines of business, including products and services. Some of these assumptions made by ZMP's algorithms (and how they appear within the ZMP platform) include:

- a. “Propensity Scores” which are ZMP data signals that score users based on their propensity to purchase a product. The data inputs it collects in order to make these assumptions are a user’s:
- i. Discretionary spending;
 - ii. Household income;
 - iii. Net-worth;
 - iv. Education completed;
 - v. Credit card usage;
 - vi. House price; and
 - vii. Number of adults in household.
- b. “Multicultural Audience Filters” which are ZMP demographic filters that allow business customers to target users based on their race or origin, specifically, if the user is African American or Black, Asian, Hispanic or Latino, or White/Non-Hispanic. The display panel for business customers to target potential consumers by race appears as follows:

The screenshot displays the 'Audience Explorer' interface for Zeta Prospects. It features a sidebar with a back arrow and the title 'Audience Explorer'. Below the sidebar, the main area is divided into four sections:

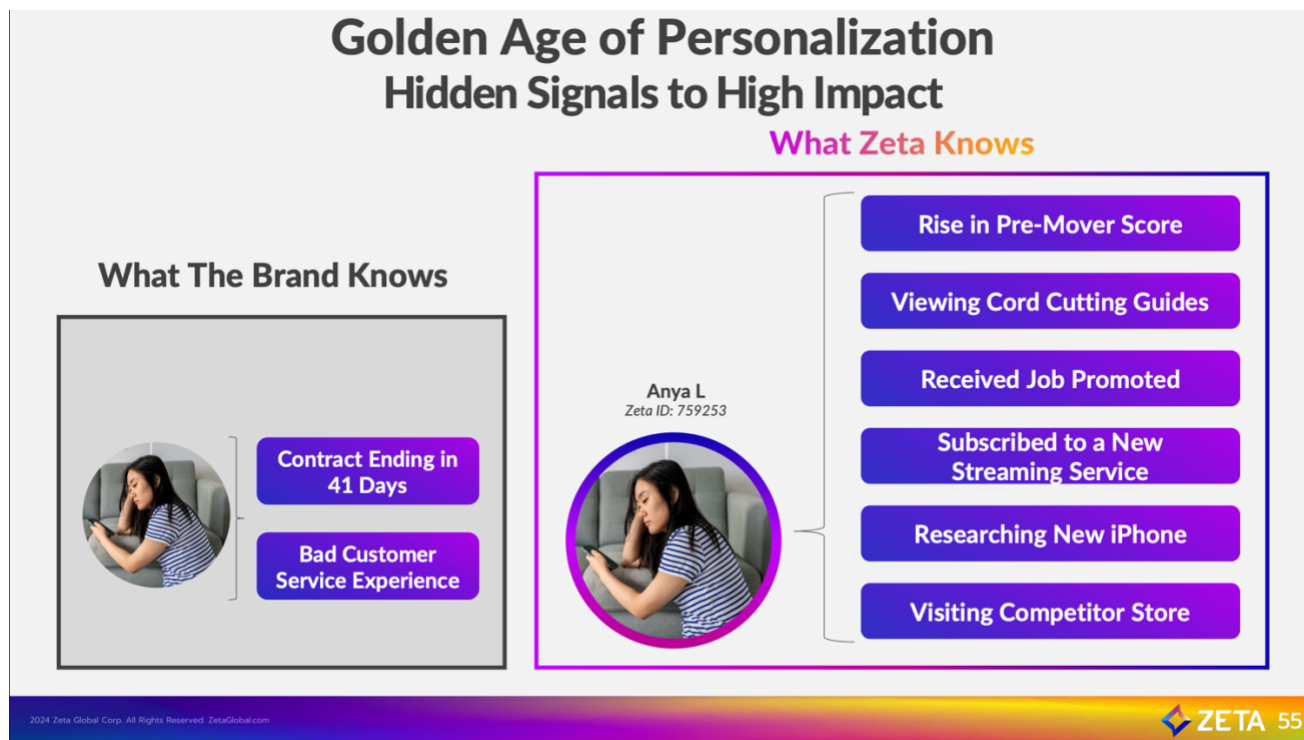
- Gender:** Includes checkboxes for 'Men' and 'Women', both of which are checked. There is also an '+ Add More' link.
- Multicultural Audiences:** Includes checkboxes for 'African American or Black', 'Asian', 'Hispanic or Latino', and 'White or Non-Hispanic White', all of which are checked.
- Age range:** A slider control with input boxes at '18' and '99'. The slider is positioned at the maximum value of 99.
- Income range:** A slider control with input boxes at '0' and '200+'. The slider is positioned at the maximum value of 200+.

The interface is clean and modern, with a light gray background and blue accents for the checked items and slider handles.

- c. “Advanced Location Targeting” which is ZMP’s ability to allow business customers to not only target potential consumers based on general geographic region, but precise location information including “city, state, zip code and longitude/latitude.”

74. Using all of this data as well as the assumptions made by ZMP’s AI systems, Defendant gives business consumers access to information that otherwise would not be possible through traditional advertising – and this is only possible because of Defendant’s willingness to disregard basic notions of privacy in an effort to enrich itself and its business customers.

75. For example, at a recent conference, Defendant discussed how assumptions could empower retailers to target specific potential consumers based on data which is not even specific to the retailer itself. This includes knowing whether a consumer is making more money than they previously did due to a job promotion, if the consumer made purchases evidencing disposable income and if the consumer is researching making additional purchases using that disposable income. A slide showing this not only discusses these assumptions, but names the consumer specifically:



76. While Defendant calls access to all of this data and the assumptions that can be made off of it the “Golden Age of Personalization,” in reality, it shows that Defendant feels more emboldened to violate basic and fundamental privacy principles.

Defendant’s Misleading Privacy Representations

77. For years, Defendant claimed that all data it collected was done so using a system of opt-in mechanisms. This means that, incredulously, Defendant wanted the public to believe that the sensitive information it had harvested on nearly every single American with internet access was given to Defendant with permission.

78. It is inconceivable that nearly every single American would willingly give over this sensitive and valuable data to be retained by Defendant so that it could be aggregated and run through algorithms so that each consumer could be targeted with various types of advertising.

79. Indeed, according to The Capitol Forum, and upon information and belief, as recently as Defendant’s 2023 Annual Report, Defendant claimed that its datasets were the

“industry’s largest opted-in data set for omnichannel marketing” which powered ZMP. Defendant has also made a slew of misrepresentations to the public about the opt-in nature of ZMP’s datasets. For example, previous Annual Reports contained similar opt-in language; additionally, promotional materials on Defendant’s website from 2022 claimed Defendant’s “database is permission-based, meaning everyone in the data cloud has opted-in.”

80. However, Defendant now walks back much of these critical privacy claims.

81. In Defendant’s 2024 Annual Report removed almost all references to ZMP’s datasets being obtained through opt-in mechanisms. At the December 2024 Zeta Data Summit, Defendant claimed it only actually had true “opt-in” permission for less than half (110 million American consumers) to collect data – and even these permissions were solely for purposes of sending email correspondence from business clients.

82. At the Zeta Data Summit, chief data officer Neej Gore stated that ZMP’s cloud includes “about 90% of the U.S. adult population on a persistent ID basis, meaning we can monitor them across the internet.” While Gore acknowledged that there were only allegedly 110 million Americans who had granted permission for email solicitations, Gore tried to parse words by claiming that “digital and email permission[s] are different.” Gore then showed a slide explaining that the requirements for digital tracking and email solicitation are different – and that digital tracking “identities, signals and identifiers” are aggregated through value exchanges by the publishers (websites or applications) which collect that data in order to “drive engagement and monetize.” This slide appeared as follows:

Digital and Email Permission Have Different Requirements

Zeta Collects Permissioned Data for Web Monitoring and Email Using Methodologies Compliant with Federal Laws, State Laws, and Self-Regulatory Programs

Zeta Data Cloud Counts as of November 2024	
US Individuals Providing Permission to Online Tracking by Agreeing to Publisher Terms of Service	245M
US Individuals Providing Permission to Email via Opt-in Action	110M

Digital Permission: Identities, Signals and Identifiers are synthesized via explicit value exchange with Publishers through which they are enabled to drive engagement and monetize.

Email Permission: Identities are synthesized via explicit opt-in from a Consumer through which they are receiving services.

© 2024 Zeta Global Corp. All Rights Reserved. ZetaGlobal.com



83. According to Professor Ari Waldman of University of California (Irvine)’s School of Law, “[c]alling your data set the largest ‘opted-in’ data set and then admitting that less than half of the people in that data set are actually opted in is a straight up lie.” This also begs the consideration of whether the opt-ins that Defendant claims to have are ones that consumers are fully cognizant and made aware of. According to Alan Butler, the Executive Director and President of the Electronic Privacy Information Center, “[Zeta’s removal of ‘opt-in’ language underscores [...] the fact that these types of purported consents to data collection are really not informed, knowledgeable, intentional choices by customers[.]”

The Quantifiable Value of Data

84. The PII, other sensitive information and assumptions made by AI is highly valuable.

85. According to Defendant, Defendant’s chief executive officer David Sternberg claimed in a November 14, 2024, investor webinar that the data collection practices Defendant

uses are comparable to Meta and Google – stating, consumers participate in a “trade of value in exchange for them signing into our ecosystem.” Steinberg continued, “[i]n 100% of the cases where we collect a consumer’s data, there’s a value exchange.” And that this value exchange consists of the monetary value of the data collected from consumers (and resold to Defendant’s business customers) in exchange for being able to do things like making comments on websites, sharing social media posts with loved ones, or applying to a job on a digital job board.

86. However, this defies logic.

87. Consumers with reasonable privacy expectations online do not get adequately and justly compensated for the data that enriches Defendant and its business customers merely because Defendant partners with the business customers who allow a respective consumer to use their website. Put simply, the significant value of a consumer’s data is not matched by the transactions that Defendant and business customers make between themselves. At bottom, commenting on digital message board or applying to an online job post does not actually or tacitly act as permission for Defendant to then monetize that data; even if it were, this does not justly compensate online users for their data nor the privacy rights they give up due to Defendant’s unlawful privacy practices.

88. The data collected both in the aggregate and on each individual consumer is highly valuable.

89. In the aggregate, Defendant has built a multibillion-dollar business based off the data it collects on consumers. Indeed, this data is so valuable that Defendant’s consumers pay significant amounts just for every rudimentary access to ZMP (usually between \$70,000 to \$110,000 per license) and then higher amounts the desire for additional data increases.

90. On an individual level, Defendant’s own chief executive officer compares ZMP’s datasets to that of Meta. According to research by DataPods, in 2023, the average revenue per user (“ARPU”) on an annual basis was approximately \$147 per profile: this means that, in a comparable data set, the value of a specific Meta user’s personal data as sold by Meta to retailers was worth about \$147 to Meta because of transactions made with business customers over a one-year period. This number increases substantially when benchmarked against the entire online advertising industry (with richer data than Meta), which values annual ARPU at about \$263 per individual online user.

91. This means that, on both an aggregated and individual level, Defendant makes a substantial amount of revenue based off the data it collects – and that the datasets themselves are quantifiable.

Plaintiffs and Class Members Have a Reasonable Expectation of Privacy

92. Internet users, like Plaintiff and Class members, do not expect to be tracked across every single one of their internet-connected devices, including on their web browsers, internet-enabled applications, connected TVs, and more. Surveys regarding online privacy reinforce this. For example, in a study by Flurry Analytics, 88% of Apple device users worldwide availed themselves of “Do Not Track” features in the hopes that their privacy rights would be protected.

93. Plaintiffs and Class members had no cognizance of and did not expect that Defendant would circumvent these protections and the desire of online consumers to remain anonymous.

94. Defendant itself is relatively unknown to almost every single user for whom it holds a data profile. By no means is “Zeta Global” a household name. Even so, Defendant made no effort to avail itself to the consumers it tracks or tracked, and there is no way Plaintiffs and Class

members would have been tracked by this unknown company, let alone that it would be used to target them across online services for profit.

95. Defendant did not have adequate consent to perform this type of omni-present, cross-device tracking using Plaintiffs' and Class members' unique identifiers, PII and other sensitive information.

96. It is recognized that this information is highly valuable – and is even more valuable given that it has resale value and value for training AI and other algorithms. Indeed, this data is instrumental to updating and improving Defendant's AI and other algorithms that identify and target unique users with advertisements.

The Harm Defendant Causes

97. The harm caused by Defendant is multifaceted.

98. Defendant violates a fundamental right to privacy that consumers have online. When a consumer enters a digital space – such as an online retail storefront or pharmacy – that consumer reasonably expects that they have the same privacy rights in that digital storefront or pharmacy as they would at a brick-and-mortar storefront or pharmacy. Defendant willingly and intentionally violates these privacy rights to profit from the data they can extract by peering over the digital shoulders of each consumer.

99. Further, the data collected from Plaintiffs and Class members is highly valuable. Defendant would not have built their multi-billion-dollar business on the transaction of this data and there would not be an entire data aggregation industry if this data had no tangible value. However, Defendant does not adequately compensate Plaintiffs and Class members for the data that they collect, retain, sell and profit from. Defendant only states that the value that Plaintiffs and Class members achieve from this scheme is that it helps each consumer better be served by

digital advertising. This is not an adequate way to compensate online consumers for the data that powers ZMP and provides tremendous profit to Defendant as a whole.

100. Taken together, the deprivation of privacy rights and the failure to compensate Plaintiffs and Class members for their data intentionally causes substantial harm to millions of Americans.

Defendant's Conduct Violates Established Data Privacy Regimes

101. Privacy laws, such as the CCPA (as well as Europe's GDPR, which is a model for many state privacy statutes), mirror the same sets of principles. The two core tenants of these principles are (1) clear user consent and (2) data minimization.

102. Defendant does neither of these. Defendant makes zero effort to ensure Plaintiffs and Class members are actually aware of where their technology is used and if Defendant has a profile on them at all. By passing the buck to shady "opt-in" mechanisms on other third-party websites, Defendant maintains plausible deniability as to whether those third-party websites even received adequate user consent. Compounding these practices is the act of Defendant powering ZMP's collection of PII, sensitive information and other AI-based assumptions through acquisition of data through data brokers. This is directly at odds with Defendant's "privacy-centric" practices made on its website, advertising materials, investor presentations and elsewhere.

103. Additionally, Defendant's creation of ever-present persistent profiles and identifiers clashes with the concept of data minimalization – which requires that data is only to be retained and stored after collection for a specific period of time in which that data usage is needed or necessary.

104. Defendant's privacy practices are a blatant disregard for consumer privacy and a departure from generally accepted privacy norms.

Tolling and Concealment

105. The earliest Plaintiffs and Class members could have discovered Defendant's conduct was shortly before the filing of this Action. Plaintiffs became aware of Defendant's conduct through communications with counsel which are protected from disclosure.

106. Plaintiffs and Class members, despite their due diligence, could not have discovered Defendant's conduct by virtue of how Defendant's technology works, Defendant's lack of adequate disclosures and the failure to be informed by Defendant that it was maintaining a data profile on each member of the Class.

107. Defendant's interception of unique identifiers, including PII and other sensitive information, as well as the assumptions made by ZMP's AI, happens inconspicuously in the background. This process is undetectable to an ordinary person; it is highly technical, and it prevents Plaintiff and Class members from discovering it.

108. Defendant had exclusive knowledge that Defendant's technology (as well as the technology used by Defendant's subsidiaries, business customers, and contracted data aggregators) were tracking Plaintiffs and Class members across the internet.

109. Defendant's fraudulent conduct prevented Plaintiffs and Class members from discovering its conduct, which began as late as January 1, 2019. Defendant made misleading representations about how all of the information it collected was done with consent or with "opt-in procedures," only for Plaintiffs and Class members to have no knowledge whatsoever that Defendant had intercepted and retained their data.

110. Defendant was under a duty to disclose the nature and significance of its data interception and use practices – especially considering its problematic false public statements –

but did not do so. Defendant, therefore, is estopped from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

111. This Action is properly maintainable as a class action pursuant to Federal Rule of Civil Procedure 23, Rules 23(a), 23(b)(1) and 23(b)(2). Plaintiffs bring this class action on behalf of themselves and all other similarly situated individuals. The nationwide class Plaintiffs seek to represent is defined as follows:

Nationwide Class. All natural persons in the United States for whom Defendant aggregated, collected, retained, sold or otherwise profited from their PII or other sensitive information.

112. In the alternative to the nationwide class, Plaintiffs seek to represent the following statewide sub-class pursuant to Federal Rules of Civil Procedure, Rules 23(a) and 23(b)(3):

New York State Sub-Class. All natural persons in the State of New York for whom Defendant aggregated, collected, retained, sold or otherwise profited from their PII or other sensitive information.

California State Sub-Class. All natural persons in the State of California for whom Defendant aggregated, collected, retained, sold or otherwise profited from their PII or other sensitive information.

113. Excluded from the Classes are (1) Defendant and Defendant's subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; (2) Plaintiffs' counsel; and (3) all judges assigned to hear any aspect of this litigation as well as their immediate family members.

114. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

115. *Numerosity.* Plaintiffs do not know the exact number of Class members because such information is in the exclusive control of Defendants or others. Plaintiffs believe that, due to

the nature of the trade and commerce involved, there are as many as 230 million Class members geographically dispersed throughout the United States, such that joinder of all Class member is impracticable.

116. *Typicality.* Plaintiffs' claims are typical of those of other Class members because Plaintiffs, like every other Class member, were harmed by way of the anticompetitive conduct as alleged herein. Plaintiffs, like all other Class members, were injured by Defendants' uniform conduct. Plaintiffs are advancing the same claims and legal theories on behalf of himself and all other Class members, such that there are no defenses unique to Plaintiffs. The claims of Plaintiffs and those of the other Class members arise from the same operative facts and are based on the same legal theories.

117. *Commonality.* There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- i. Whether Defendant violated Plaintiffs' and the Classes' privacy rights;
- ii. Whether Defendant engaged in unfair and deceptive conduct;
- iii. Whether Defendant's acts and practice violate the California Invasion of Privacy Act;
- iv. Whether Plaintiffs and Class members are entitled to damages and/or equitable relief, including injunctive relief, restitution, and disgorgement of profit into a constructive trust;
- v. Whether Defendant was unjustly enriched; and
- vi. The appropriate class-wide measure of damages as well as whether Plaintiffs and Class members are entitled to such damages and other relief.

118. *Adequacy of Representation.* Plaintiffs will (and has) fairly and adequately represent and protect the interests of the Class members in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights that Plaintiffs suffered are typical of other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in data privacy class action litigation, and Plaintiffs intend to prosecute this action vigorously.

119. *Superiority of Class Action.* A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class' common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

120. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

121. Adequate notice can be given to Class members directly using information maintained in the parties' records.

122. *Predominance.* The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

123. This proposed class action does not present any unique management difficulties. Defendants have acted on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole.

FIRST CAUSE OF ACTION

VIOLATION OF NEW YORK’S GENERAL BUSINESS LAW § 349

ON BEHALF OF THE NATIONWIDE CLASS, OR, ALTERNATIVELY, THE NEW YORK
STATE SUB-CLASS

124. Plaintiffs reallege and repeats each and every allegation from paragraphs 1-122 as if fully realleged and set forth herein.

125. Defendant is considered a business under New York’s General Business Law § 349 (“GBL § 349”).

126. Defendant’s business acts and practices are unfair and deceptive under GBL § 349. New York (as do other states through their respective unfair and deceptive trade practices statutes) has a strong public policy of protecting consumers’ online privacy rights, including online personal data. Defendant violated GBL § 349 by, among other things, surreptitiously aggregating, collecting, retaining, selling and otherwise profiting from Plaintiffs’ and Class members’ PII and other sensitive information. Defendant used tracking technology to track Plaintiffs’ and Class members’ activities on all websites containing Defendant’s tracking technology to create user profiles for Plaintiffs and Class members’ as part of its advertising business.

127. Defendant’s business acts and practices are also “unfair” in that they are immoral, oppressive, unscrupulous and/or substantially injurious to consumers. The gravity of harm of Defendant’s secret collection and use of consumer PII for advertising purposes is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs and

Class members were completely unaware of Defendant's conduct, they could not have avoided these harms.

128. By collecting and using Plaintiffs' and Class members' PII, Defendant has taken money or property from Plaintiffs and Class members and caused harm to Plaintiffs' and Class members' privacy interests. Plaintiffs and Class members seek all available damages under all substantially similar applicable state consumer protection laws, including statutory damages of \$50 per violation for each Class member under GBL § 349.

SECOND CAUSE OF ACTION

VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")

ON BEHALF OF THE CALIFORNIA STATE SUB-CLASS

129. Plaintiffs reallege and repeats each and every allegation from paragraphs 1-122 as if fully realleged and set forth herein.

130. CIPA § 631 prohibits any person who, but means of any "machine, instrument or contrivance" or in "any other manner": (1) intentionally taps or makes an unauthorized connection with "any telegraph or telephone wire, line, cable or instrument;" (2) willfully and without consent of "all parties to the communication" or in "any unauthorized manner" reads or "attempts to read" or "learns the contents or meaning of any message, report or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place" within California; (3) "uses or attempts to use, in any manner, or for any purposes, or to communicate in any way" information so obtained; or (4) from aiding, agreeing, employing or conspiring with "any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

131. Defendant is a person under CIPA § 631.

132. Defendant intercepted Plaintiffs' and Class members' unique identifiers and other personal data and private communications while "in transit or passing over any wire, line or cable or is being sent from, or received from any place within" California.

133. At all relevant times, Defendant used its technology to make unauthorized connections with the lines of communication and instruments used by Plaintiffs and Class members to access online services without the consent of all parties to those communications.

134. Defendant willfully, and without consent, read, or attempted to read, or learn the contents and meaning of Plaintiffs and Class members communications with online services while those communications were in transit or passing over a wire, line, or cable, or were being sent or received within California through its tracking technology, as described herein. This interception happens prior to or at the same time that they would be received by the intended recipient.

135. Defendant used and attempted to use these identifiable, private communications without consent for its own benefit, including for targeted advertising.

136. Plaintiff and Class members have been harmed because of Defendant's conduct. Their PII and sensitive information has been intercepted, viewed, and used for targeted advertising and has not been destroyed. Plaintiffs and Class members face an imminent threat of continued injury, as this data is still stored and used, such that Plaintiffs and Class members have no adequate remedy at law.

137. Plaintiffs and Class members seek statutory damages in accordance with CIPA § 637.2(a) which provides the greater of: (1) \$5,000 per violation or (2) three times the amount of damages suffered by Plaintiffs and Class members in an amount to be proven at trial, as well as equitable and injunctive relief.

THIRD CAUSE OF ACTION

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

ON BEHALF OF THE NATIONWIDE CLASS

138. Plaintiffs reallege and repeats each and every allegation from paragraphs 1-122 as if fully realleged and set forth herein.

139. The Electronic Communications Privacy Act (“ECPA”) makes it illegal to intentionally intercept, or attempt to intercept, any wire, oral, or electronic communication and to disclose or use the contents of an unlawfully intercepted communication. 18 U.S.C. § 2511.

140. ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

141. Defendant intentionally intercepted electronic communications that Plaintiffs and the Class members exchanged with Defendant through the tracking tools installed on Defendant’s business customers’ websites.

142. The transmission of data between Plaintiffs and the Class members and Defendant qualifies as communications under ECPA. 18 U.S.C. § 2510(12).

143. Defendant contemporaneously intercepted and transmitted Plaintiffs’ and the Class members’ communications of that data to the advertising technology companies whose trackers Defendant installed or allowed to be installed on its website.

144. The tracking mechanisms that Defendant uses to track Plaintiffs’ and the Class members’ communications, Plaintiffs’ and the Class members’ browsers, Plaintiffs’ and the Class members’ computing devices, and the code that Defendant placed or allowed to be placed on its website, are all “devices” within the meaning of 18 U.S.C. § 2510(5).

145. The online retail companies that are the recipients of communications between Plaintiffs and Class members, on the one hand, and Defendant, on the other, are not party to those communications.

146. Defendant transmits the contents of those communications through the surreptitious redirection of the communications from Plaintiffs' and the Class members' computing devices.

147. Plaintiffs and Class members did not consent to the ad tech companies' acquisition of their communications with Defendant. Nor did the ad tech companies receive legal authorization to receive such communications.

148. In disclosing the content of Plaintiff's and Class members' communications relating to the purchase and use of Defendant's products, Defendant had a purpose that was tortious, criminal, and designed to violate statutory and constitutional privacy provisions including:

- a. The unauthorized disclosure of PII is tortious, regardless whether the means deployed to disclose the information violates the ECPA or any subsequent purpose or use;
- b. Intrusion upon Plaintiffs' and the Class members' seclusion;
- c. Trespass upon Plaintiffs' and the Class members' personal and private property; and
- d. Violation of 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy) which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in

interstate ... commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice.”

149. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were used. Penalties apply to attempts as well as offenses. 18 U.S.C. § 1349.

150. Defendant’s scheme or artifice to defraud consists of the false and misleading statements in its privacy policy described herein.

151. Defendant acted with intent to defraud in that it willfully invaded and took Plaintiffs’ and Class members’ property, including the property rights to their PII and their right to determine whether such information remains confidential; the right to determine who may collect and use such information for marketing; and the right to determine who has access to their devices and communications.

152. Defendant also acted with intent to defraud in that it willfully invaded and took Plaintiffs’ and Class members’ property (their PII) with knowledge that it lacked consent or authorization to do so; a reasonable consumer would not understand that Defendant was collecting and transmitting their data to third parties; a reasonable consumer would be shocked to realize the extent of Defendant’s disclosure of data to third parties; and the subsequent use of health information for marketing was a further invasion in that the use was not related to any healthcare.

153. Defendant acted with the intent to acquire, use, and disclose Plaintiffs’ and Class members’ PII and PHI without their authorization or consent.

154. Plaintiffs and Class members have suffered damages because of Defendant’s

violations of ECPA, including that (1) Defendant eroded the essential, confidential nature of the relationship between Defendant and its customers, (2) Defendant failed to provide Plaintiffs and Class members with the full value of the services for which they paid, which included a duty to maintain confidentiality and protect privacy, (3) Defendant derived valuable benefits from using and sharing Plaintiff's and Class members' communications without their knowledge or informed consent and without providing compensation, (4) Defendant's actions deprived Plaintiffs and Class members of the value of their PII, (5) Defendant's actions diminished the value of Plaintiffs' and Class members' property rights in their PII; and (6) Defendant violated Plaintiffs' and Class members' privacy rights by sharing their PII for commercial use.

155. Plaintiffs and Class members seek appropriate declaratory or equitable relief including injunctive relief, actual damages and profits enjoyed by Defendant because of violations or the appropriate statutory measure of damages, punitive damages, and reasonable attorneys' fees and costs. 18 U.S.C. § 2520. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class members seek monetary damages for the greater of (i) the sum of the actual damages suffered by the plaintiff and any profits made by Defendant because of the violation or (ii) statutory damages of whichever is greater of \$100 a day for each violation or \$10,000.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT

ON BEHALF OF THE NATIONWIDE CLASS

156. Plaintiffs reallege and repeats each and every allegation from paragraphs 1-122 as if fully realleged and set forth herein.

157. Defendant received benefits from Plaintiffs and Class members and unjustly retained those benefits at their expense.

158. Defendant received benefits from Plaintiff and Class members in the form of the Plaintiffs' and Class members' highly valuable data, including PII, that Defendant wrongfully collected, disclosed and intercepted from Plaintiffs and Class members without authorization and proper compensation.

159. Defendant collected, disclosed, intercepted, stored, and used this data for their own gain, providing Defendant with economic, intangible, and other benefits, including highly valuable data for analytics, advertising, and improvement of their platforms, algorithms, and advertising services.

160. Had Plaintiffs and Class members known of Defendant's misconduct, they would not have provided any of their valuable data the applications or websites which Defendant used for aggregation or would have paid less for the services on those applications or websites.

161. Defendant unjustly retained these benefits at the expense of Plaintiffs and Class members because Defendant's conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs and Class members.

162. The benefits that Defendant derived from Plaintiffs and Class members rightly belong to Plaintiffs and Class members. It would be inequitable for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Action.

163. Defendant should be compelled to disgorge profits into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

DEMAND FOR RELIEF

164. To remedy these illegal acts, Plaintiffs request the following relief:
- a. Certify the Classes and appoint Plaintiffs as the Classes' representatives;
 - b. Declaring, finding, adjudging and decreeing that the conduct of Defendant is unlawful and violates the federal and state law;
 - c. Disgorging Defendant's profits from their unlawful data privacy scheme into a constructive trust;
 - d. Awarding to Plaintiffs the costs of their suit, including reasonable attorneys' fees;
 - e. Awarding to Plaintiffs their damages, in the amount to be determined by a jury, inclusive of statutory and/or treble damages as provided by the applicable federal and state laws;
 - f. Granting to Plaintiffs and Class any such and other relief to which they may be entitled and which this Court deems just and proper.

JURY TRIAL DEMANDED

165. Plaintiffs demand a trial by jury on all claims so triable under Federal Rule of Civil Procedure Rule 38(b).

[The Remainder of this Page is Intentionally Blank]

Dated: July 15, 2025

Respectfully submitted,

By: /s/ Blake Hunter Yagman

Blake Hunter Yagman

Michelle C. Clerkin

SPIRO HARRISON & NELSON

40 Exchange Place, Suite 1100

New York, New York 10005

Tel.: (929) 709-1493

Fac.: (973) 232-0887

byagman@shnlegal.com

mclerkin@shnlegal.com

Christian Levis

Amanda Fiorilla

LOWEY DANNENBERG, P.C.

44 South Broadway, Suite 110

White Plains, New York 10601

Tel.: (914) 997-0500

Fac.: (914) 997-0035

clevis@lowey.com

afiorilla@lowey.com

Israel David

ISRAEL DAVID LLC

60 Broad Street, Suite 2900

New York, New York 10004

Tel.: (212) 350-8850

Fac.: (212) 350-8860

israel.david@davidllc.com

Counsel for Plaintiffs and the Proposed Class